Photo courtesy of the Ashland County Sheriff's Office

R-TECH™ NEWSLETTER
The Newsletter of the First Responder Technologies Program

Volume 3 • Issue 2 • February 2010

To contact R-Tech
E-mail: RTech@DHS.gov

IN THIS ISSUE

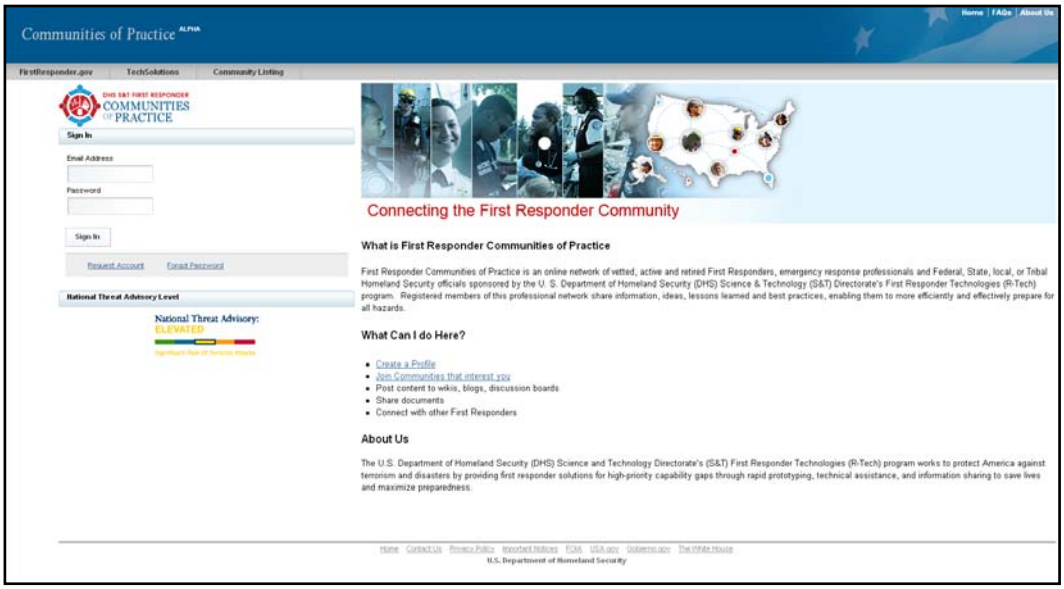
Homeland Security
Science and Technology

This Newsletter discusses technologies of interest to first responders that have received funding, in part, from the Federal government. Mention of these technologies should not be construed as an endorsement of either the technology, or the entity producing it, by the Federal government.

COMMUNITY CONNECTIONS

First Responders and Homeland Security Officials Collaborate in a Virtual Community

First responders can collaborate on department policies or homeland security projects easily when they all work in the same office and shift. When they work in different shifts, disciplines, offices, cities, or states, the task grows more complex. To encourage improved collaboration and partnerships, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) First Responder Technologies (R-Tech) program created a virtual platform where first responders and federal, tribal, state, or local homeland security officials can communicate, network, and collaborate on team projects and critical homeland security initiatives. R-Tech formally launched the Alpha version of the online platform, called First Responder Communities of Practice, at the Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition in Philadelphia in February 2010.



Communities of Practice, a virtual workspace developed by the First Responder Technologies (R-Tech) program, offers first responders a place to network and collaborate on projects. Image courtesy of DHS S&T.

Communities of Practice is a nationwide network of vetted first responders (active and retired) and homeland security officials. Members of this professional network share information, innovative ideas, lessons learned, and best practices, enabling them to more efficiently and effectively prepare for all hazards. Registered members can post their profile to aid in networking with members who have similar interests or backgrounds. They also can set up their own communities on the platform to work on specific projects, according to R-Tech Program Manager Jeff Hudkins.

"It's a virtual collaboration platform that allows first responders across the nation to connect with each other around common interests or initiatives," Hudkins said. "[Members] can work together collaboratively using the platform, which takes advantage of the social networking capabilities."

The Communities of Practice platform can help organizations, departments, and teams unify their visions through intra- and inter-agency sharing and collaboration across projects and initiatives. Through this networking and project collaboration platform, first responders can increase awareness and transparency of their work with homeland security stakeholder groups across the country, strengthen and build partnerships, leverage knowledge and resources, facilitate information exchanges, and allow collaboration on critical homeland security projects. As a result, work across distances and times will be streamlined, and costly duplication of resources and efforts can be greatly reduced.

Hudkins explained that the secure collaboration platform provides several capabilities: threaded discussions, document repositories, blogging, group calendars, and other next-generation Web tools designed to help first responder groups and organizations with their team projects. For example, members who need other members to edit a document could post a draft in their particular community, and members could use the platform's wiki tool to leave comments or make changes to the draft. Each member can edit the document when it is convenient for them, and the revisions are saved in a central location everyone can access. The system

Community Connections (continued)

eliminates the need for a member to combine many revisions into a single document, according to Hudkins. "Everyone can touch [a document] and make it a little better," he said. "Over time, the product evolves into a more robust, more mature [document]."

Five groups experimented with a pilot version of Communities of Practice that R-Tech established in December 2007. In 2008, the New York City Fire Department (FDNY) set up a community and subgroups on the pilot platform for about 80 firefighters and emergency management partners, according to Lt. Tony Mussorfiti, who works at the FDNY Center for Terrorism and Disaster Preparedness. FDNY and its partners used Communities of Practice to plan tabletop training and disaster preparedness exercises. They also used the online community to draft best practice documents for FDNY. Using the community to stay in touch between face-to-face meetings helped the members collaborate efficiently, according to Mussorfiti. "This gave us the ability to stay in communication with other agencies in the city in the building of [tabletop exercises]," he said. "You didn't have to have as many conference calls and face-to-face meetings."

Communities of Practice provides homeland security professionals and first responders an online platform where they can collaborate. Photo courtesy of the U.S. Customs and Border Patrol.

Once members of FDNY's community became familiar with the platform, Mussorfiti said they appreciated its benefits. Communities of Practice made it easier for many people to offer input on a project, Mussorfiti noted.

First responders who use Communities of Practice can be assured that they are communicating with vetted colleagues and government officials, Hudkins said. Prospective users must be vetted through a process that involves contacting a sponsor to verify his or her status as a first responder or homeland security official. Active and retired first responders and federal, tribal, state, and local homeland security officials may request a Communities of Practice account at www.Communities.FirstResponder.gov.

R-Tech is developing a Beta version of the site that will incorporate additional features and improvements, according to Hudkins. R-Tech plans to continue rolling out improvements to the platform to enhance its functionality and benefit first responders and homeland security officials. Communities of Practice members will help chart the platform's future course and influence how it develops.

As part of R-Tech's broader effort to provide useful online resources for first responders, R-Tech also plans to launch a redesigned version of FirstResponder.gov – a comprehensive Website providing access to federal resources for first responders – during the first quarter of 2010. FirstResponder.gov catalogues Weblinks to federal information on first responder grants, equipment certification standards, testing, and much more. The online portal provides a comprehensive list of federal resources for first responders in one place, according to Hudkins. The redesigned site features a blog highlighting DHS projects that support first responders and articles about emerging first responder technologies. The new Website, which is scheduled to be launched in the first quarter of 2010, will be easier for first responders to navigate and quickly find the information they need, according to Hudkins.

For more information, visit www.FirstResponder.gov.

SIFTING THROUGH DATA

Software Tracks Illegal Computer Activity

When police hunt for evidence of a crime in which a computer is believed to be involved, the investigation often requires officers to dig through a huge amount of data, looking for the proverbial needle in a haystack. Finding and interpreting clues that pinpoint a suspect's activities is time consuming and requires specialized knowledge. These clues, however, can provide valuable evidence in court. To aid in these efforts, a software program called P2P Marshal – available for free to law enforcement agencies nationwide – speeds up the process of discovering and documenting illegal file-sharing activity, a common means of distributing illegal software and images.

P2P Marshal searches for peer-to-peer file-sharing software that has been downloaded to a computer and creates a list of the files swapped in each program. Child pornographers and other criminals commonly use peer-to-peer software programs such as BitTorrent and LimeWire to obtain and distribute photographs, videos, and other illegal material online. P2P Marshal can retrieve evidence of that activity within minutes, according to Dr. Frank Adelstein, technical director of computer security for ATC-NY, a subsidiary of Architectural Technology Corp. that created the P2P Marshal software.

The software, funded by the Department of Justice's National Institute of Justice (NIJ), debuted in early 2008. Version 2.1 was released in September 2009, according to ATC-NY. The latest version analyzes a suspect computer for activity in several peer-to-peer software programs. P2P Marshal provides a full analysis of files shared in Ares, BitTorrent, FrostWire, LimeWire, µTorrent, and Vuze. The program also can detect and show default download locations for Kazaa files. Without the software, forensic investigators would need to be familiar with each of the seven peer-to-peer software programs, as well as variations in different versions, to perform that same analysis, and it would likely take hours, Adelstein said. Using P2P Marshal saves time and allows officers to investigate more cases. "They have more work than they have time to deal with," he said.

The majority of the cases investigated by the Broome County Government Security Division's Computer Analysis & Technical Services Unit (CATS), based in Binghamton, N.Y., involve child pornography, said Jim Thompson, the unit's supervising forensic analyst. CATS offers video and computer forensic services to six counties in upstate New York. "Roughly between 78 to 88 percent of our case intake involves child exploitation," he said. "This tool speeds up the triage of these kinds of cases."

The P2P Marshal software can document files shared using peer-to-peer clients in 10 to 15 minutes, according to Thompson, who uses the software routinely. It would take CATS staff about two hours to create a similar report without the software. Moreover, the time required for computer forensic analysis is growing longer as time passes, due to ever-larger inexpensive data storage devices reaching the market. "The volume of what we're taking in is such that it has completely taxed the most valuable resource we have, which is trained personnel," Thompson said.

Officers learn to search for illegal computer files using the P2P Marshal software during a training session. Photo courtesy of ATC-NY.

Officers investigating child pornographers want to move quickly to detain suspects and prevent them from committing additional crimes, according to Thompson. If forensic analysis finds evidence of child pornography files on a suspect's computer, federal prosecutors can use that information to seek pre-trial detention of a suspect.

In addition to detecting peer-to-peer software and past activity, P2P Marshal also documents the IP addresses of anyone with

Sifting Through Data (continued)

whom the suspect traded files. Officers can use the IP address information to locate other suspects who could be creating or sharing child pornography, according to Martin Novak, physical scientist for NIJ at the Department of Justice's Office of Justice Programs, which funded the software's development. Even if a suspect uninstalls peer-to-peer software to avoid detection, P2P Marshal can find traces of past activity, according to Novak, including traces of files that never finished downloading.

The P2P Marshal Website, http://p2pmarshal.atc-nycorp.com, explains how law enforcement agencies can obtain a free copy of the software. Photo courtesy of ATC-NY.

NIJ has sponsored training classes to show state and local first responders how to use P2P Marshal, according to Judson Powers, principal scientist for ATC-NY. Understanding what evidence can be obtained from a computer and how to interpret it is essential to using P2P Marshal effectively, and that is a major focus of the training, added Adelstein. ATC-NY, which conducts the courses, demonstrates how police can use the program to obtain evidence, prepare forensic reports, and support court testimony. ATC-NY organizes one-day training courses for interested law enforcement groups across the country.

State and local law enforcement agencies nationwide can obtain a free copy of P2P Marshal from ATC-NY. The instructions are available at http://p2pmarshal.atc-nycorp.com/p2p/download.html. For more information, visit http://p2pmarshal.atc-nycorp.com, or www.ojp.usdoj.gov/nij.

LENDING LIBRARY

Robot Loan Program Allows First Responders to Test Models

When bomb squads invest thousands of dollars to purchase robots, officers want to ensure the equipment will meet their needs. Different models offer different capabilities, and many first responders prefer to run training exercises with specific robots to determine if they are good fits for their department. The Space and Naval Warfare Systems Command (SPAWAR) Systems Center Pacific operates a Robotic Systems Pool that offers first responders the chance to borrow a robot and learn how it functions before making a significant investment.

SPAWAR Systems Center Pacific has an inventory of about 50 robots to loan to bomb squads, Special Weapons and Tactics (SWAT) teams, and other first responders who want to use them in training exercises, according to Navy Capt. Mike Carter, the Center's Project Officer for Department of Defense (DoD) Technology Outreach Centers. This equipment is also available to DoD agencies, academic partners, and companies developing related technologies. The RSP gives first responders and other users access to robots that have seen action in Iraq, new models just off the production line, and even experimental systems for advanced technology development.

Borrowers do not pay for use of the robots, according to Carter. "The whole idea was to provide essentially a free resource," he said. The Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs helps support the program as part of a broader DoD effort to share defense technology with first responders. Through the DoD Technology Outreach Centers, many other kinds of equipment have been made available to first responders in addition to robots. The inventory includes night vision devices, handheld language translators, personal chemical detectors, and personal decontamination kits.

Lending Library (continued)

When DoD established the program in 2002, it primarily provided robots to train military personnel being deployed to Iraq, according to Carter. Since 2005, the program has shifted that focus to provide technology developed for DoD to the first responder community. For example, police borrow robots to use during tactical training exercises to determine the quality of surveillance they might provide during a simulated hostage situation.

The RSP is working to make robots and other equipment more readily available to first responders through the outreach centers, according to Carter. SPAWAR Systems Center Pacific set up the first outreach center at the Public Safety Academy of Northeast Indiana, a first responder training facility that opened in Fort Wayne, Ind. in November 2007. A new center recently opened at the Massachusetts State Police Academy in New Braintree, Mass., and another is planned for Barbers Point, Hawaii.

Much of the demand for loaned robots comes from bomb squads. The Federal Bureau of Investigation (FBI) requires bomb squads to have a robot or they risk losing the FBI certification that allows them to operate. Before making a purchase, bomb squads can borrow a model from the RSP to evaluate which ones will meet their needs. "They get to make a smart decision on how they spend their money," Carter said. Moreover, Carter explained that participating first responders provide SPAWAR Systems Center Pacific feedback on the borrowed equipment, which is shared with manufacturers to improve future generations of robots.

The Ashland County Sheriff's Office in Ohio uses a borrowed robot during a training exercise. Photo courtesy of SPAWAR Systems Center Pacific.

The Robotic Systems Pool loaned this Vanguard MK II robot to the Ashland County Sheriff's Office in Ohio for bomb squad training. Photo courtesy of the Ashland County Sheriff's Office.

Large robot designs featuring the latest technological advances can cost up to $250,000, said Capt. Mike Kyle, bomb squad commander for the Ashland County Sheriff's Office in Ohio. The Ashland-based regional bomb squad, which serves six counties in northern Ohio, is applying for grants and other financing to enable it to purchase a robot. To gain experience, the department borrowed a Vanguard MK II robot equipped with a manipulator arm with wrist and claw camera as well as two-way audio, from the RSP during the second half of 2009. The six-month loan allowed the bomb squad to put the machine through its paces, Kyle said. One training exercise required officers to direct the 130-pound robot up a flight of stairs to search school classrooms for a simulated improvised explosive device (IED). "The main thing is it allows a bomb squad that doesn't have a robot to get good hands-on experience with a robot," he said.

With a robot in their equipment arsenal, bomb squads can disable an explosive without physically approaching it, according to Kyle. The robot's camera allows bomb squad members to examine a suspected explosive without risking injury. After taking a close look, bomb squad members can then determine the best course of action for

Lending Library (continued)

disarming the device. The robots can assist in this as well. For example, many bomb-disposal robots are armed with water cannons capable of disrupting an explosive's wiring without setting off an explosion. "It gives us the ability to approach [an explosive] remotely," he said.

Robots have broader applications for emergency response beyond bomb squad use, according to Kyle. Hazmat disposal teams can use robots to examine chemical spills from a remote location. SWAT teams rely on robots for surveillance and establishing communication with suspects holding hostages. Some robots can be equipped to deliver tear gas and other non-lethal weapons.

When first responders use robots during tactical maneuvers, it minimizes the risk to police officers. It is better for a robot to be damaged by an IED than to have a police officer or soldier risk injury, according to Jim Fallin, director of corporate communications and public affairs at SPAWAR Systems Center Pacific. "In my view, there's no more poignant message or example than to get a robot back and know that robot represents a saved life or multiple saved lives," he said.

The RSP continues to add to its inventory and expects to receive about 10 more robots in upcoming months, according to Carter. SPAWAR Systems Center Pacific recently added two Segway-based robots that could be used for search-and-rescue operations to the RSP.

The Ashland County Sheriff's Office in Ohio borrowed this robot from the Robotic Systems Pool for bomb squad training. Photo courtesy of SPAWAR Systems Center Pacific.

For more information on the RSP, visit www.publicsafetyacademy.org/dod-technology-outreach-center. For more information on robot technologies, read the September 2008 Special Robot Edition of the R-Tech Newsletter posted at www.firstresponder.gov/NewsLetters/September%202008.pdf.

RESPONDER KNOWLEDGE BASE

P25 on RKB

Stemming from the need for a common set of standards for digital radio communication, the Association of Public-Safety Communications Officials – International (APCO), the National Association of State Technology Directors (NASTD), and several federal agencies established Project 25 (P25). P25 encompasses a suite of standards for public safety radios to improve equipment interoperability and compatibility.

As a trusted resource for equipment-related information, the Responder Knowledge Base (RKB), located at www.rkb.us, posts information on P25-compliant technology and standards. In collaboration with the Department of Homeland Security Science and Technology Directorate (DHS S&T) Office for Interoperability and Compatibility (OIC), RKB has created a section on its Website for manufacturers to

RKB (continued)

publish data from the P25 Compliance Assessment Program (CAP), a voluntary program whereby communications equipment manufacturers can demonstrate that their equipment meets P25 standards, aiding responders in making informed procurement decisions. DHS S&T announced on Jan. 14, 2010 that the first land-mobile radio had completed the P25 CAP process. P25 standards make it possible for radios to interoperate regardless of manufacturer, enabling emergency responders to communicate more effectively. The first radio to complete the P25 CAP compliance process is the P5400 800MHz P25 conventional/trunked unit produced by Harris Corporation.

To complete this process, radios must be tested by laboratories that have been recognized through a rigorous and objective assessment process based on internationally-accepted standards. P25 CAP has formally recognized eight laboratories – Compliance Testing LLC; EF Johnson Technologies; Motorola ASTRO System Integration & Test Laboratory; Motorola GP25 HEC-PITEC Schaumburg; Motorola P25 Performance CAI Subscriber Compliance Laboratory; Tait Electronics Ltd. Teltest Laboratories; TIMCO Engineering Inc.; and RF Communication Division, Harris Corporation – to conduct a predetermined set of tests on P25 products. These tests determine product compliance and interoperability with a select group of conformance, performance, and interoperability tests within the suite of P25 standards. Through RKB, manufacturers can post summary reports of the test results and a Supplier's Declaration of Compliance (SDoC). These documents are linked to the manufacturer's product information on the RKB, if it is listed. Manufacturers began posting P25 product information on the RKB in December 2009.

The creation and maintenance of a company's P25 compliance information on RKB will be the responsibility of the manufacturer. Once provided, the summary reports and SDoCs will be available in the Certifications and Declarations section of RKB.

For more information on how to add or access these P25 documents on RKB, please email RKBMailbox@us.saic.com or call 1-877-FEMA-RKB (1-877-336-2752).